BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(11) **DE 3441724 A1**

(51) Int. Cl. 4:
H 04 Q 7/02
H 04 L 11/26
H 04 Q 3/70
H 04 K 1/00

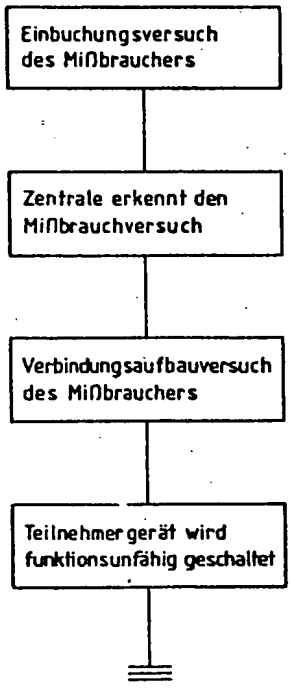
(21) Aktenzeichen: P 34 41 724.9
(22) Anmeldetag: 15. 11. 84
(43) Offenlegungstag: 15. 5. 86

(71) Anmelder:
Siemens AG, 1000 Berlin und 8000 München, DE

(72) Erfinder:
Diederich, Hans G., Dipl.-Ing.; Logemann, Helmut, 6100 Darmstadt, DE

(54) Verfahren zur Mißbrauchsverhinderung in Fernmeldenetzen, insbesondere Mobilfunknetzen

Um den Mißbrauch von Teilnehmergeräten durch computergestütztes Ausprobieren von geheimen Kennungen in zellularen Mobilfunknetzen zu erschweren, erfolgt bei einem bereits während des Einbuchungsvorgangs für die Zentrale erkennbaren Mißbrauchsversuch zunächst keine für den Mißbraucher erkennbare besondere Reaktion der Zentrale. Die Kennung des nicht zugangsberechtigten Teilnehmergerätes wird aber in der Zentrale gespeichert. Erst bei einem der folgenden Verbindungsaufbauversuche reagiert die Zentrale für das Teilnehmergerät erkennbar, indem sie entweder die gewünschte Verbindung nicht herstellt oder die zunächst hergestellte Verbindung nach einer bestimmten Zeit unterbricht. In beiden Fällen kann anstelle der gewünschten Verbindung eine Ansage zum Teilnehmergerät gesendet werden. Alternativ dazu wird das nicht zugangsberechtigte Teilnehmergerät von der Zentrale für wenigstens eine bestimmte Zeit funktionsunfähig geschaltet. Die Abschaltung kann entweder irreversibel sein, dann muß ein besonderer Baustein des Teilnehmergerätes ausgetauscht werden, oder dieser Baustein kann mitt Is einer besonderen Vorrichtung wieder funktionsfähig geschaltet werden. Beides bleibt dem Netzbetreiber vorbehalten (Fig. 5).



DE 3441724 A1

Deutsche Bundespost 2580

Umgeschrieben

3441724

Verfahren zur Mißbrauchsverhinderung in Fernmeldenetzen, insbesondere Mobilfunknetzen

(9) Patentansprüche

1 Verfahren zur Mißbrauchsverhinderung in Fernmeldenetzen, insbesondere in aus mehreren Teilnehmergeräten und wenigstens einer Zentrale bestehenden zellularen Mobilfunknetzen, in denen jedes Teilnehmergerät vor dem eigentlichen Verbindungsaufbau wenigstens einen Einbuchungsvorgeng durchläuft, der zur Aktualisierung von im Netz geführten Dateien dient und bei dem in der Zentrale anhand der empfangenen Kennung des Teilnehmergerätes dessen Zugangsberechtigung festgestellt wird, d a d u r c h g e k e n n z e i c h n e t , daß seitens der Zentrale im Falle des Erkennens eines nicht zugangsberechtigten Teilnehmergerätes zunächst keine besondere für das Teilnehmergerät erkennbare Reaktion erfolgt, die Zentrale aber die Kennung des nicht zugangsberechtigten Teilnehmergerätes speichert und erst bei einem der folgenden von ihm ausgehenden Verbindungsaufbauversuche für das Teilnehmergerät erkennbar reagiert.

2 Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die erkennbare Reaktion der Zentrale im Nichtherstellen der gewünschten Verbindung besteht (Fig. 1).

3 Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die erkennbare Reaktion der Zentrale im Unterbrechen der zunächst hergestellten Verbindung nach einer bestimmten Zeit besteht (Fig. 2).

4 Verfahren nach Anspruch 2 oder 3, dadurch gekennzeichnet, daß anstelle der gewünschten Verbindung eine Ansage zum Teilnehmergerät gesendet wird (Fig. 3 und 4).

...

Deutsche Bundespost 2580

5 Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die erkennbare Reaktion der Zentrale in einer Fernabschaltung des nicht zugangsberechtigten Teilnehmergerätes besteht (Fig. 5).

6 Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß der Zustand der Funktionsunfähigkeit der bei einem Mißbrauchsversuch abgeschalteten Tln-Geräte irreversibel ist und den Austausch eines besonderen Bausteins erfordert, in dem alle zur Durchführung der Abweisstrategie erforderlichen Funktionseinheiten in integrierter Bauweise zugriffssicher zusammengefaßt sind.

7 Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß die bei einem Mißbrauchsversuch abgeschalteten Teilnehmergeräte durch eine besondere Vorrichtung in den funktionsfähigen Zustand zurückversetzt werden können.

8 Verfahren nach Anspruch 6 oder 7, dadurch gekennzeichnet, daß der Austausch des Bausteins oder die Zurückversetzung in dem funktionsfähigen Zustand allein vom Netzbetreiber vorgenommen werden können.

9 Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß die die Fernabschaltung des mißbräuchlich benutzten Teilnehmergerätes beim ersten Verbindungsaufbauversuch erfolgt.

...

 Umgeschrieben

Zur Legitimation eines Zugangsberechtigten zu einem gegen fremdem Zugriff geschützten Fernmeldesystem werden den Zugangsberechtigten entweder zusätzlich zu einer offenen Identifikation geheime Kennungen oder ein/mehrere Schlüssel zur verschlüsselten Übertragung der offenen Identifikation zugeordnet. Es ist auch das Verfahren bekannt, die zu übertragenden Kennungen mit Scheininformation zu mischen (verschleiern). Geheime Kennungen, Schlüssel und die entsprechenden Verfahrensparameter sind nur den jeweils Zugangsberechtigten bekannt und in wenigstens einer Zentrale in Dateien gespeichert.

Da offene Identifikationen, Schlüssel (parameter) und die gesamte sonstige Signalisierung auf einem ungeschützten Nachrichtenkanal übertragen werden, besteht die Gefahr, daß ein potentieller Mißbraucher durch Anzapfen bzw. Abhören Eigenschaften des Signalisierungsverkehrs erkennt, auswertet und mittels eines manipulierten Teilnehmergerätes durch Probieren (Browsing) schließlich doch , obwohl nicht autorisiert, Zugang zum Netz als vermeintlich Zugangsberechtigter erhält. Diese Gefahr wächst beträchtlich durch die Verfügbarkeit marktgänger Personal- und Home-Computer.

Aufgabe der Erfindung ist es, den Zeitaufwand für den einzelnen Probierversuch durch besondere Abweisstrategien dadurch zu verlängern, daß der Mißbraucher (Probierer) möglichst lange über den Erfolg bzw. Mißerfolg im Unklaren gehalten wird.

Bei modernen, zellularen Mobilfunksystemen wird jedes mobile Teilnehmergerät beim Hineinfahren in eine Funkzone bzw. erstmaligen Einschalten mit seiner Kennung in der Zentrale gespeichert. Dies geschieht zwangsläufig, ohne daß das Teilnehmergerät einen Verbindungswunsch zu äußern braucht. Diese Vorgänge werden mit "Ein-", "Um-" und "Ausbuchen" bezeichnet und dienen u.a. der Leitweglenkung bei für das Teilnehmergerät bestimmten Verbindungen.

...

Deutsche Bundespost 2580

Beim Ein- oder/und Umbuchen wird in den bekannten Systemen die Zugangsberechtigung überprüft und bei fehlender Zugangsberechtigung das Teilnehmergerät sofort abgewiesen. Für den Mißbraucher wäre es einfach möglich, mit Hilfe eines Personal- oder Home-Computers diese Einbuchversuche zu automatisieren und ohne eigenes Zutun innerhalb kürzester Zeit durchzuführen.

Hier setzt die Erfindung wie folgt ein:
Der erkannte Einbuchungsversuch des Mißbrauchers führt nicht unmittelbar zum Ausbuchen oder zur Abweisung des nichtzugangsberechtigten Teilnehmergerätes. Der Mißbraucher wird somit gezwungen, will er sich Klarheit über den Erfolg seines Versuchs verschaffen, im Anschluß an diesen Einbuchungsversuch eine Verbindung aufzubauen, um dann an der Reaktion des Fernmeldenetzes erst erkennen zu können, ob sein Einbuchungsversuch wirklich erfolgreich war. Auch bei einer Automatisierung der Einbuch- und anschließenden Verbindungsaufbauversuche würde der erforderliche Zeitaufwand um mehrere Größenordnungen über dem liegen, der bei den heute im Betrieb bzw. in der Planung befindlichen Mobilfunksystemen erforderlich wäre.

Die Teilnehmergeräte moderner Fernmeldenetze sind sehr komplex. Es wird in Zukunft nicht mehr oder nur unter großen Schwierigkeiten möglich sein, z.B. die Funktion von Teilnehmergeräten in einem zellularen Mobilfunksystem mit breitbandig digitaler Modulation mit heute üblichen Meßsendern und Meßempfängern nachzubilden. Ein modernes Teilnehmergerät in solchen Fernmeldenetzen stellt eine höchstintegrierte funkspezifische Datenverarbeitungs-Anlage dar. Der Mißbraucher wird also nicht umhin können, sich ein solches zugelassenes Teilnehmergerät zu beschaffen und es zum Zwecke des Probierens zu manipulieren.

Mehrere Ausführungsbeispiele der Erfindung, welche die Wirkungsweise der Verhinderung erfolgreicher Mißbrauchsversuche verdeutlichen, sind in 5 Ablaufdiagrammen dargestellt.

Es zeigen

Fig. 1 den Ablauf beim Ausbleiben des Verbindungsaufbaus ohne weitere Maßnahmen von Seiten der Zentrale

Fig. 2 die Unterbrechung der zustande gekommenen Verbindung

Fig. 3 die Durchschaltung einer Ansage zum Teilnehmergerät des Mißbrauchers anstelle des Verbindungsaufbaus

Fig. 4 die Durchschaltung einer Ansage erst nach erfolgtem Verbindungsaufbau

Fig. 5 die Funktionsunfähigschaltung des Teilnehmergerätes des Mißbrauchers

Im Beispiel der Fig. 1 erkennt die Zentrale den Einbuchungsversuch des Mißbrauchers, speichert die dabei benutzte Kennung ab und behandelt den Mißbraucher so, als sei sein Versuch nicht als Mißbrauch erkannt worden. Der Mißbraucher baut eine Verbindung auf und erst jetzt benutzt die Zentrale ihre Kenntnis und ignoriert den Verbindungsaufbauwunsch des Mißbrauchers. Dieser wartet eine zeitlang (eine Zeit, die üblicherweise zum Verbindungsaufbau im Fernsprechnetz und zur Durchschaltung im Funknetz erforderlich ist), erkennt schließlich das Scheitern seines Versuchs und wiederholt ihn, beginnend mit der Einbuchung, mit einer geänderten Kennung.

In Fig. 2 wird der versuchte Verbindungswunsch des Mißbrauchers zunächst ausgeführt; er glaubt sich am Ziel, aber nach einer bestimmten Zeit unterbricht die Zentrale diese Verbindung. Er wird im Laufe der Zeit merken, daß es sich dabei um keine Fehlfunktion des Netzes oder Unterbrechung als Folge von Abschaltung der Funkwellen handelt sondern, daß sein Versuch erkannt wurde. Er kann also nur die Kennung seines Teilnehmergerätes ändern und mit dem Einbuchen einen neuen Mißbrauchsversuch beginnen.

In Fig. 3 wird bei sonst gleichem Ablauf nach dem Verbindungsaufbauversuch des Mißbrauchers eine Ansage zu seinem Teilnehmergerät durchgeschaltet. Dabei kann es sich bei der "Ansage" um ein Geräusch o.ä. handeln, das eine Fehlschaltung vortäuscht, oder um einen Text, der den erkannten Mißbrauchsversuch gezielt anspricht.

...

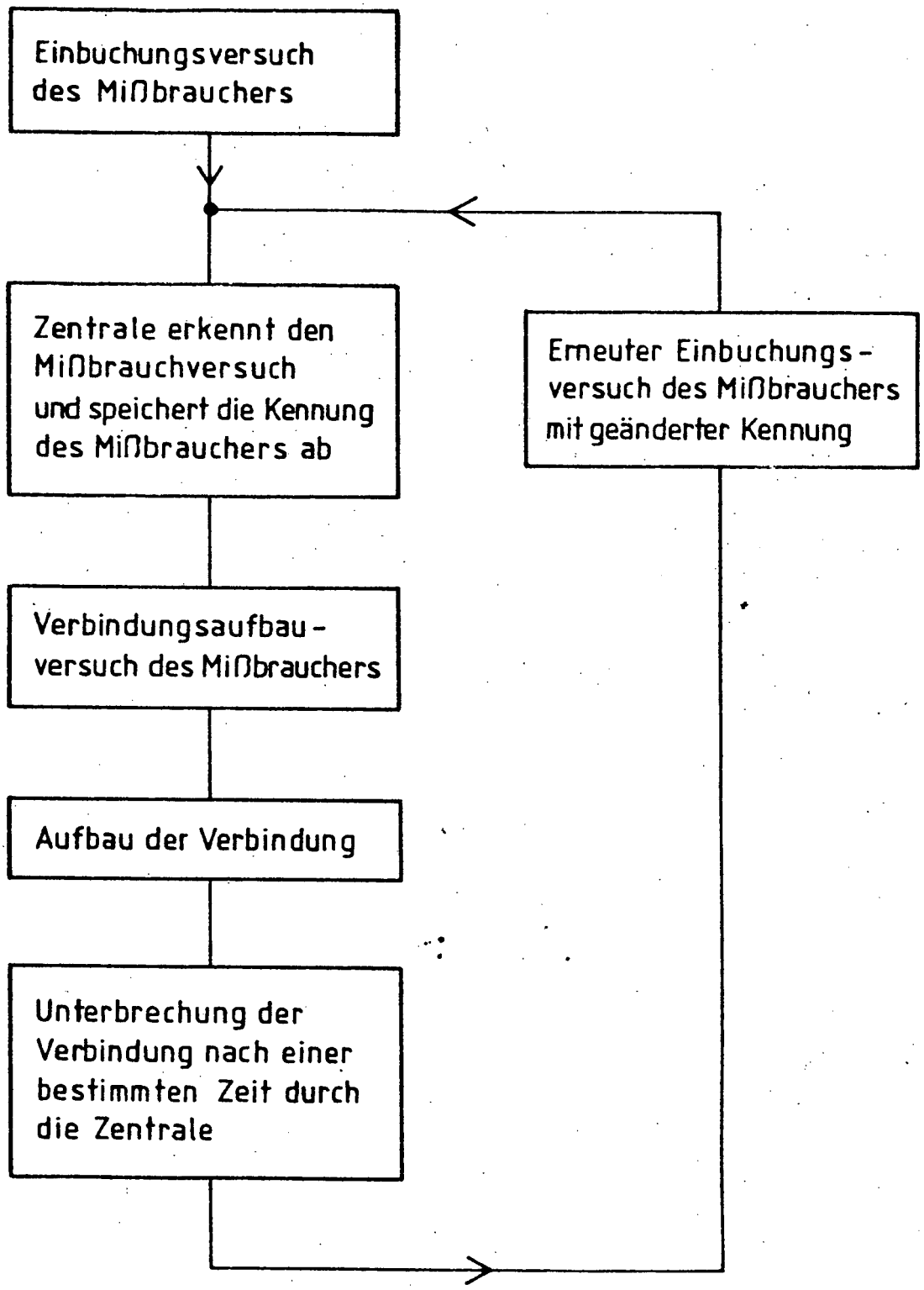
In jedem Fall bleibt dem Mißbraucher zur Wiederholung des Mißbrauchsversuches nur ein neuer Versuch mit geänderter Kennung übrig, der nur mit dem erneuten Einbuchen beginnen kann.

Die Fig. 4 erläutert eine Variante , die darin besteht, daß im Anschluß an den Verbindungsaufbauversuch die Verbindung zwar aufgebaut wird, die zustandegekommene Verbindung jedoch unterbrochen und an ihrer Stelle eine Ansage zum Teilnehmergerät durchgeschaltet wird. Der Mißbraucher kann wiederum nur mit geänderter Kennung und beginnend mit der Einbuchung seinen Mißbrauchsversuch wiederholen.

Fig. 5 erläutert die stärkste Reaktion der Zentrale auf einen Mißbrauchsversuch. Der Mißbraucher bucht sich zunächst ein. Die Zentrale, seinen Mißbrauch erkennend, speichert die benutzte Kennung ab und führt den Signalisierungsverkehr zum Teilnehmergerät derart durch, daß der Mißbraucher im Glauben gelassen wird, der erste Schritt seines Mißbrauchsversuches sei geglückt. Wenn er aber seinen Verbindungswunsch eingibt, wird eine im Teilnehmergerät vorhandene Vorrichtung nach Erkennung der Nichtzugangsberechtigung durch die Zentrale dieses Teilnehmergerät funktionsunfähig schalten. Weitere Mißbrauchsversuche (Probierversuche) sind damit unterbunden. Soll das Teilnehmergerät wieder in den funktionsfähigen Zustand zurückversetzt werden, muß eine autorisierte Stelle des Netzbetreibers aufgesucht werden. Will der Mißbraucher sich nicht der Gefahr der Erkennung seiner Gerätemanipulation aussetzen, bleibt ihm nichts anderes übrig, als sich ein anderes Teilnehmergerät zu beschaffen.

Alle sicherheitsrelevanten Funktionseinheiten sind in einem integrierten Baustein zugriffssicher untergebracht. Dies erschwert bzw. verhindert Manipulationen (z. B. Außerkraftsetzung ihrer Schutzfunktionen).

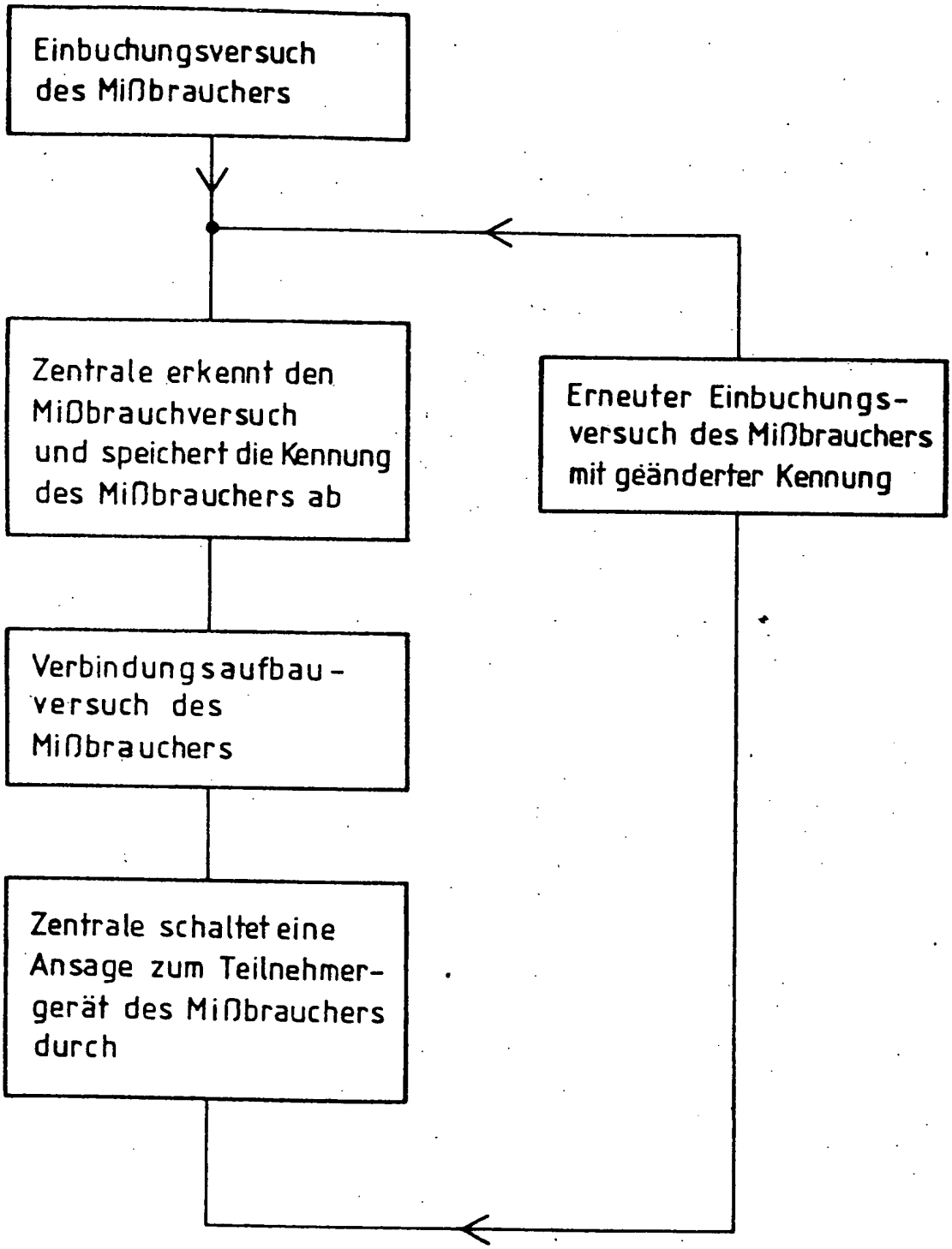
Fig. 2



Unterbrechung der zustande gekommenen Verbindung

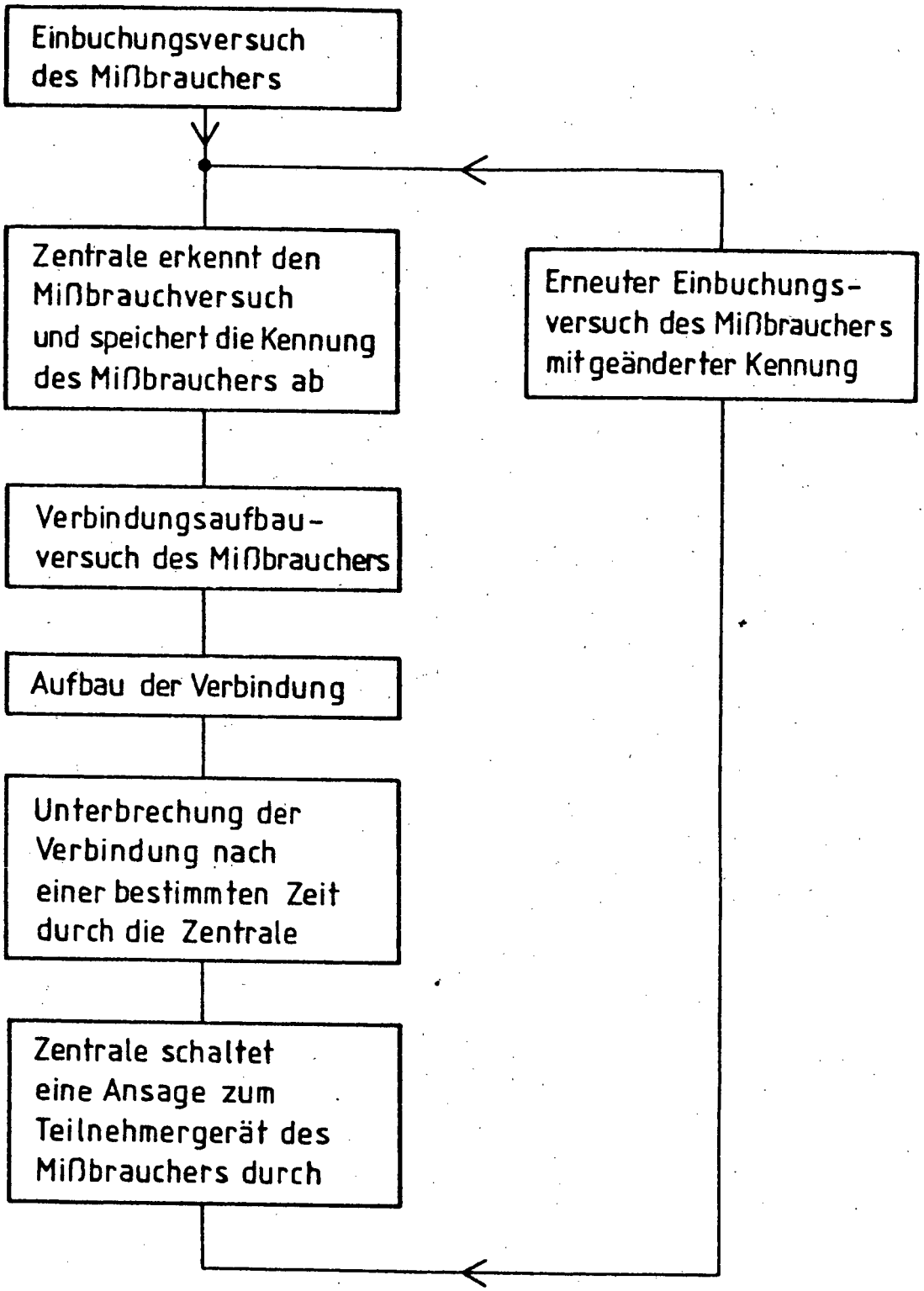
Deutsche Bundespost 2580

Fig. 3



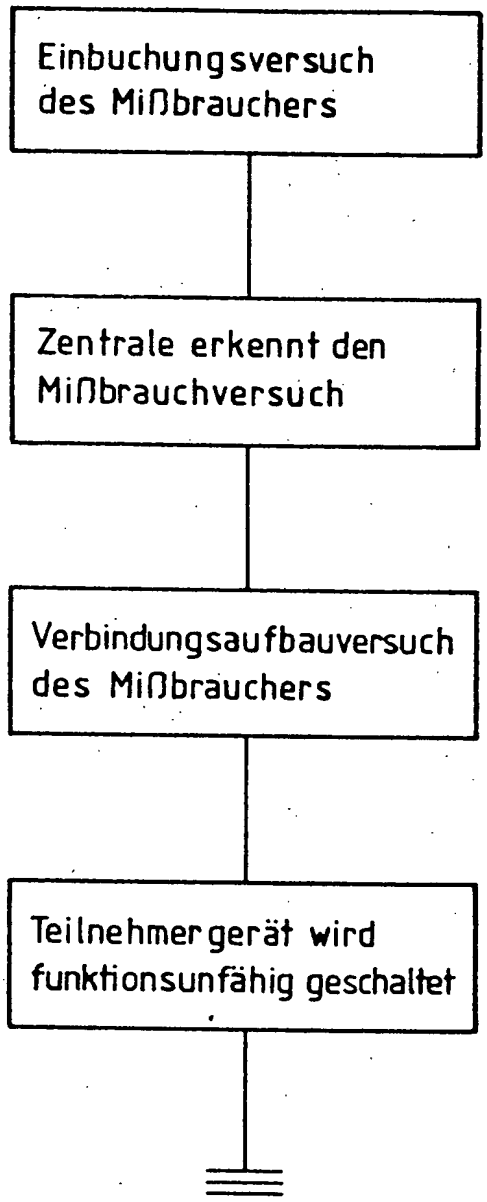
Durchschalten einer Ansage zum Teilnehmergerät

Fig. 4



Durchschalten einer Ansage erst nach erfolgtem Verbindungsaufbau

Fig. 5

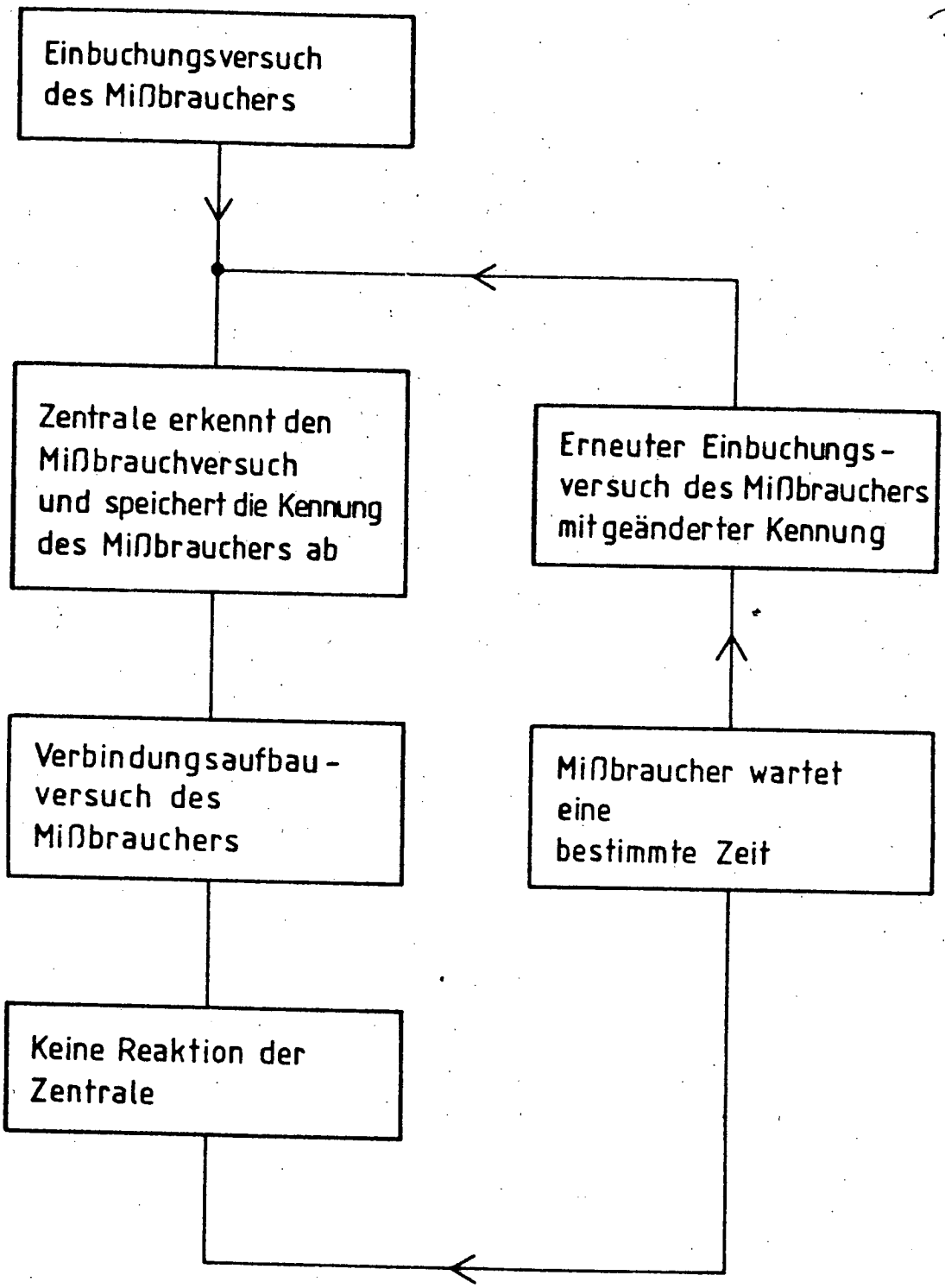


Funktionsunfähigschalten des Teilnehmergerätes

Nummer: 3441724
Int. Cl.4: H 04 Q 7/02
Anmeldetag: 15. November 1984
Offenlegungstag: 15. Mai 1986

H04L
~~44-26~~
72/22

Fig. 1



Ausbleiben des Verbindungsaufbaus ohne weitere Maßnahme